UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/552,951	04/20/2000	Zheng Jia	9344-0004-999	6045

20583 7590 12/24/2003

PENNIE AND EDMONDS
1155 AVENUE OF THE AMERICAS
NEW YORK, NY 100362711

EXAMINER	
CURCIO, JAMES A F	
ART UNIT	**PAPER NUMBER**
2132	8

DATE MAILED: 12/24/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/552,951	JIA ET AL.	
	Examiner	Art Unit	
	James Curcio	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 April 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 April 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *6, 7*.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Drawings

1. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "106" has been used to designate both a critical function profile and an obscure code bank and reference character "401" has been used to designate both a transformation function and an encryption processor. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: 204. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: 105, 212, 403, 404, and 812. A proposed drawing correction, corrected drawings, or amendment to the specification to add the reference sign(s) in the description, are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

4. The drawings are objected to because elements 602 and 601 should be 601 and 602 respectively, in accordance with the detailed description. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

5. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: Obstructing Code Insertion to Prevent Reverse Engineering and Tampering of Computer Data or Software.

6. The disclosure is objected to because of the following informalities. On page 11, line 21, "form" should be spelled "from." On page 12, line 14, "207" should be "206." On the same page, line 17, "collections" should be "collection." On page 13, line 7, "transportation" should be "transformation." On page 16, line 22, "can executed" should be "can be executed."

Appropriate correction is required.

Claim Objections

7. Claim 14 objected to because of the following informalities: second instance of "comprising" is not a step. The remainder of the office action interprets this instance of "comprising" as "compressing". Appropriate correction is required.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

9. Claims 1-20 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter that was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The specification fails to enable the production of "an obscured sequence of computer instructions that in total is humanly impossible to read and understand". Rather, a human can read and understand the claimed invention's obscured sequence of computer instructions after a significant amount of time and processing (see page 8, line 28 and page 9, line 13). In the remainder of this office action, I interpret the words "in total is humanly impossible" in base claims 1, 10, and 19 as "is difficult".

10. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 10, and 19 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The term "large" in claims 1, 10, and 19 is a relative term which renders the claim indefinite. The term "large" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the

invention. The remainder of this office action will interpret the word "large" in claims 1, 10, and 19 with the broadest reasonable interpretation.

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-7, 10-15, and 18-21 rejected under 35 U.S.C. 102(b) as being anticipated by Aucsmith et al (US5892899A).

12. As per claims 1, 10, and 19, Aucsmith et al discloses the preparation of obscuring instructions (column 1, lines 46-57; column 4, lines 16-20; column 5, lines 38-46; column 7, lines 9-15 and 23-25), the injection of these obscuring instructions into computer code to form an obscured sequence of instructions (column 1, lines 46-57; column 4, lines 16-20; column 5, lines 38-46; column 7, lines 9-15 and 23-25), and the encryption of a static image of this sequence (column 10, lines 62-65). These steps are taught as being combined on a computer system and an embedded controller in two example embodiments (column 11, lines 42-47 and lines 66-67; column 12, lines 1-3), and this office action interprets the obscured sequence of instructions generated as comprising the instructions taught in all of these steps combined.

13. As per claims 2 and 20, in addition to the teachings applied above, Aucsmith et al discloses the execution of obscured instructions one instruction at a time (column 5, lines 32-33 and column 9, lines 41-43).

14. As per claims 3 and 11, in addition to the teachings applied above, Aucsmith et al discloses the association of obscuring instructions and a first set of codes (see "pseudo-randomly selected pattern(s) of mutations" and "one or more ordered sets of pseudo-random keys" in column 5, lines 38-46). Aucsmith et al also discloses the transformation of a first set of codes into a second set of codes (see the method of choosing mutations by cycling through the pseudo-random keys in column 5, lines 38-46). The invention also discloses the generation of a second set of obscuring instructions (see "obfuscated subprograms cyclically mutate" in column 5, lines 38-46).

15. As per claims 4-5 and 12-13, in addition to the teachings applied above, while Aucsmith et al fails to expressly disclose that the first set of codes is a set of numeric codes, the "pseudo-random keys" (column 5, lines 38-46) are encoded in a computer system (column 3, lines 28-33) and therefore are inherently represented with binary numbers. Likewise, the transformations in Aucsmith et al are mathematical because transformations of binary numbers on a computer system are inherently mathematical.

16. As per claims 6-7 and 14-15, in addition to the teachings applied above, Aucsmith et al also discloses the step of compressing the static image by recording a record of the transformation used to generate the second set of

obscuring instructions (See working matrix M2 containing Boolean functions to recover the plaintext of the obfuscated subprograms in column 6, lines 57-64. This matrix is a compressed form of the record of transformation).

17. As per claim 21, in addition to the teachings applied above, Aucsmith et al also discloses an obscuring obstruction bank (see "pattern(s) of mutations" in column 4, lines 16-20; column 5, lines 37-38 and lines 40-41; column 7, lines 9-16 and 23-25), a transformation function bank (see "predetermined mutation partnership function" in column 5, lines 39-41), and a generator (see the method of choosing mutations by cycling through the pseudo-random keys in column 5, lines 38-46).

Claim Rejections - 35 USC § 103

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 8-9 and 16-17 rejected under 35 U.S.C. 103(a) as being unpatentable over Aucsmith et al (US5892899) as applied respectively to claims 1 and 10 above, and further in view of Bellare et al (US5673319A).

19. As per claims 8-9 and 16-17, in addition to the teachings applied above, Aucsmith et al discloses the organization of the obscured sequences of computer instructions into a sequence of blocks of computer instructions (see "obfuscated subprograms" in Aucsmith et al column 1, lines 58-51 and column 5, lines 20-22), the encryption of a static image of the obscured sequence of instructions (column

10, lines 62-65), and the compression of the static image by recording a record of the transformation used to generate the second set of obscuring instructions (Aucsmith et al, column 6, lines 57-64) but fails to expressly disclose the encryption of a first block of obscured instructions to form a first encrypted output, the encryption of a second block and first encrypted output to form a second encrypted output, and the encryption of a third block and the second encrypted output to form a third encrypted output. However, Bellare et al discloses these features in a Cipher Block Chaining encryption algorithm (Bellare et al, column 1, lines 48-60; column 2, 42-45; and claim 3). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Aucsmith et al to encrypt each obfuscated subprogram using the cipher block chaining encryption algorithm disclosed in Bellare et al as the Boolean expressions representing the obfuscation procedures in compressed form are recorded in matrix M2. One of ordinary skill in the art would have been motivated to do so in order to hide or secure plain-text instructions in the obfuscated subprograms from malicious users (see Bellare et al, column 1, lines 10-26, 37-40, 48-60 and column 2, lines 42-45).

20. Claims 22 and 23 rejected under 35 U.S.C. 103(a) as being unpatentable over Aucsmith et al (US5892899). Aucsmith et al, in a second aspect of a tamper resistant method, discloses a plurality of critical instructions (see "security sensitive program in column 5, lines 20-22) and obscuring instructions (column 7; lines 16-25). Aucsmith et al also discloses a step for executing loading

instructions to allocate a first dynamic memory address, which implies a step for loading such instructions (see "jump block" in column 6, lines 19-22; figure 4, elements 201, 202, and 204; and figure 5, element 209). It also discloses a step for loading and executing critical instruction(s) (see subprograms" and "executions" in column 5, lines 30-34). These steps repeat using a step-wise incremented loading instruction blocks, dynamic memory addresses, and critical instructions (i.e. first, second, and third block of loading instructions loaded and executed at a first memory address and first, second, and third critical instructions loaded and executed at respective first, second, and third dynamic memory addresses) until all "jump blocks" are exhausted (i.e. loaded and executed) and all subprograms are loaded and executed (See "jump block" in column 6, lines 19-22 and figure 5, element 209, and see the ellipsis separating the dynamically chosen memory locations where critical instructions are loaded and executed in figure 4, elements 201, 202, and 204).

Aucsmith et al's first aspect fails to expressly disclose two decryption keys, the steps of retrieving the first and second decryption keys, and the steps of decrypting the second and third blocks of loading instructions respectively using the first and second decryption keys.

However, Aucsmith et al's fifth aspect discloses these features: the decryption keys (see K_p^{pvt} and K_c in column 11, lines 13-24), the retrieval steps for the keys (see "using its own" in column 11, line 18 and "recovered" in column 11, lines 22-23), the decrypting steps (see decryption of Kp^{pub}[Kc] and Kc[cntnt] in column 11, lines 13-24).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Aucsmith et al's first aspect by encrypting each subprogram before distribution and decrypting each subprogram during execution with retrieved decryption keys corresponding to each subprogram in a manner equivalent to the features described in Aucsmith et al's fifth aspect.

One of ordinary skill in the art would be motivated to do so in order to render the subprograms virtually impossible to modify while located on insecure platforms (see Aucsmith et al column 1, lines 26-30).

Conclusion

21. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

a. Folmsbee, Alan (US-6609201B1)

b. Chow et al (US-6594761B1)

c. Granger et al (US-6480959B1)

d. Johnson et al (US-5748741A)

e. Nardone et al (US-6175925B1)

f. Drake, Christopher Nathan (US-6006328A)

g. Schwartz et al (US-6006328A)

h. Ostrovsky et al (US-5123045A)

i. Moore, Steven Jerome (US-6067622A)

j. Best, Robert M (US-4465901)

k. Jackson, Andrea Ontko (US-6662361B1)

l. Burns, Ronnie R. (US-5940129A)

m. Collberg, Christian, Clark Thomborson, and Douglas Low. "Manufacturing Cheap, Resilient, and Stealthy Opaque Constructs. January 1998. http://www.cs.arizona.edu/~collberg/Research/Publications/

n. Benson, Greg et al (WO-00/34845)

o. Nardone, Joseph et al (WO-99/13613)

p. Nardone et al (US-6178509B1)

q. Candelore et al (US-6061449)

r. Maliszewski (US-6049609)

s. Drake (US-6006328)

t. Jia et al (US-5991402)

u. Collberg, Christian et al (WO-99/01815

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Curcio whose telephone number is 703-305-8887. The examiner can normally be reached on Tuesday through Friday from 7:00 am – 5:30 pm.

23. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached at 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

24. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

JC
December 11, 2003

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100